Social Engineering Using Phishing

Anant Singhal – 16BCI0159
Department of CSE,
Vellore Institute of Technology,
Vellore
Slot: C2

Sai Teja – 16BCI0209
Department of CSE,
Vellore Institute of Technology,
Vellore
Slot: C2

Abstract— **Phishing Attacks are the most common type of network attacks faced by the organizations as well as the individuals worldwide. In this attack, the attacker creates a similar file like a webpage of an existing website from scratch or by using various website scraping tools also known as phishing tools which make a duplicate of the website and then the attacker hosts this duplicate webpage to fool and extract the online users into giving the elicit personal information to the attacker. The prime objective of this paper is to show how social engineering can be performed using phishing by several and very common different ways using various phishing tools to make phishing websites and host them to perform social engineering.**

***Keywords*— Social Engineering Attacks; Phishing Attacks; Phishing Tools; Personal Data;**

I. Introduction

The one of the main objectives of Information Security is to deal with the protection of the sensitive information from the social engineering attacks like the various phishing attacks, money laundering, privacy of sensitive data etc. In Social Engineering attack, the attacker is trained in the art of manipulating the common people who don't have much knowledge about the security and technology into revealing the desired personal information that he wants. Every, specialists as well as the users in order to protect the personal and sensitive data from such kind of social engineering attacks.

Phishing is one of the most serious threat in the world of limitless service of internet. There are many ways discovered by the attackers to trick the people into revealing or disclosing the required information by social engineering attack. Social engineering can be performed onsite as well as offsite. Phishing attack is one of the most common offsite social engineering attacks. In this attack, the attacker lures the user by sending mails that the user has won a prize, or may send messages on social networking sites from fake accounts, sending emails which seems to be sent by the victim's bank, making fraud calls to the victim being a bank representative and asking the victim about his credit card details for financial gain. Phishing is considered to be the most dangerous and sophisticated threat in the world. In 1995, the first phishing incident encountered. The mass of users were targeted in the password stealing scam on the website of America Online (AOL). The software used was AOHell. Since then, the phishing threats have increased and developed.

According to the Global Phishing survey published by APWG, specified that "there were at least 12 ,741 unique phishing attacks worldwide in the first half of 2014". Phishing attacks, in which users deceived by scam emails and bogus websites, to reveal sensitive information such as passwords, "social security number", credit card details, or other personal information. Basically Phishers use social engineering techniques to target their victims, these techniques include the human factors of psychology and sociology. Cybercriminals combine human factors with technology factors to gain the trust of victim by gathering some information about their regular activity such as shopping history, which can be available in many websites such as eBay, or other available information sources , this technique called "context aware phishing" . Social networks such as Facebook and Twitter have become a decent source for phishers, social network data can be exploited, which can expand the harvest of phishers . Criminals can use crawling sites tools such as promptcloud.com where social media site canb e used to obtain data and convert this data into" structured format e.g. XML" [ ]. Phishing is simply committed with very little effort, EMC published a fraud report in January 2014, estimated that the losses in 201 for phishing in the UK with "$467 million", also the report mentioned that "over 62 ,000 unique phishing attack identified in a single month". [4]. Obviously this report reflects how serious the problem of phishing threats, phishing attack can cause financial losses, and critical security breaches. Phishers have developed new techniques to target a specific organization or group of selected targets, this technique is called "spear phishing" [5]. Spear phishing technique uses email fraud to target a particular organization, to gain unautherised access to sensitive information [5] . Spear phishing attacks target intellectual property, energy sector, or government services. New method of phishing attack such as "watering hole" attack which is used by attackers to infect victims with zero-day malware, mostly the attackers select a website in a specific sector to compromise.

Phisher sends messages, links, spoofed emails or even make fraud calls to millions of the users in the hope that a few of them will believe it and will fall prey to it. They mostly target people who don't have much knowledge about such online internet attacks and they make the victims believe that the spoofed email, website, link, message or call is coming from the true organization. Attackers makes all the arrangements in such a manner that everything looks professional and the users are often easily targeted and befooled.

This paper consists of four sections. First section consists of introduction; section 2 illustrates Literature Survey and types of Phishing attacks, Section   explains widely Prevention from Social engineering attacks, Section 4 explains Analysis on social engineering attacks detection techniques, followed by Conclusion in Section 5.

II. Literature Survey

Social Engineering is a combination of psychology and engineering, it is the most successful methodology used to acquire sensitive information and exploit security systems . In board computer security terms, Social Engineering can be loosely described as ”a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures”[7]. Linearly 1990s the term Social Engineering popularized by the formal computer hacker Kevin Mitnick, who is now trusted security consultant [8]. The human factor is weakest link in the security system in a corporation, social engineers target an employee to obtain sensitive information, or steer the target to take specific actions in order to exploit security system in an organization [9].When an attacker plans to target an organization, initially he/she takes in mind several factors such as the complexity of security systems, the cost of launching and deploying that attack, and the time needed to accomplish the attack successfully. Social Engineering techniques allow the attackers to breach security system with less complexity, cost effective and less time. Social Engineering attacks can be classified into two main categories, ”human-based deception and technology-based deception” [10]. Human-based deception method can be performed by study the ”human factors psychology and sociology, these factors include human error, external influences, management, policy issues, and training” [11]. Attackers seek for security gaps in these factors, to indirectly obtain sensitive information about a system, for example an attacker impersonates the manager role, he emails the IT help desk in an organisation, and he asks the help desk person to resets the password and provides the new password to him. Technology-based deception method is to deceive the user into believing that he is interacting with the real service and ultimately get him to expose confidential information[10], for example email attachment, popup windowand so forth. Technology-based deception method is rapidly rising with the new emerging web applications such as social networks, and online services. Basically technology-based deception is the most dangerous approach, it allows attackers to bypass any security layer which created to defend against cyber threats. Social engineering can take many forms and techniques, one of the most common source of social engineering is phishing technique, according to Dimensional Research survey on social engineering threats in 2011 indicated that ”phishing threats were identified as the most typical source for social engineering of 47%, followed by social networking sites such as LinkedIn” [12] . This paper will focus on phishing techniques, the new forms of phishing threats, and the defence approaches. The term Phishing refers to ”the process of tricking or socially engineering an organisations customers into imparting their confidential information for nefarious”[1].Early Internet hackers used email lures to ”phish” confidential information such as passwords and financial data from the ocean of the Internet . The word phishing was popularised in ”1996 by hackers who were stealing America Online (AOL) accounts by scamming passwords from unsuspecting AOL users” [1], AOHell was the first software innovated by hackers to steal confidential information, this was the first automated phishing system[14]. Since then the phishing attacks have been expanded and developed into more sophisticated fraud techniques. Nowadays the Internet has expanded to involve online transactions such as banking, shopping, and etc. according to policy paper of the UK cabinet office indicated that ”82% of adults use online services in the UK; these services include online banking, shopping, and government services”[15]. Unfortunately this grow in the online services has been accompanied with new sophisticated phishing attacks, attackers now ”expanded into fake websites, installation of Trojan horse keyloggers, and man-in-the-middle data proxies and other malicious software”[1]. Previously phishers typically were using emails as channel to interact with their victims, now phishers are using new channel to propagate their frauds for example instant messaging services, fake website, and IRC channels. Not surprisingly phishers are still using traditional approaches such as voice phishing (Vishing) to lure victims by telephone call or voice message to visit rogue website, similarly a victim can receive a SMS phishing via his smartphone, this approach called Smishing[16] .

Moreover phishers engineered the latest mass emailing techniques to distribute their fraud to a wide number of users. Phishers have the ability to manipulate DNS for a corporate website (trusted website) and redirect that website to point to a fake website, this technique known as DNS poisoning, sometimes referred to pharming. If a victim receives an officially email that seem to be sent by his bank or corporate, the content of that email asks him to click on the official website link to change his password account for some security reasons, then the victim will be more confident and perhaps will trust this website, these techniques improve the quality of hacker deception and increase the chance of success with very low risk[17]. Phishing also use Botnets to send out emails, according to a report published in 2004 by Cipher Trust ”suggested that 70% of monitored phishing spam was sent through one of five active botnets”[17]. Phishing through port redirection technique, initially the attacker scans vulnerabilities on legitimate http server, once server exploited the attacker installs a port redirection service (port redirector utility) on the server, which will be used to re-route http requests sent to the legitimate server to another remote web server. Therefore any incoming traffic on http port 80 will transparently forwarded to an attackers remote server, then an attacker starts to send off phishing emails to the legitimate servers users[17]. Most of the new phishing attacks are Malware-based phishing, this type of phishing attacks download malicious software to the victims machines, these software can be used by the phisher to steal sensitive data, gain unauthorised access to the victims machines, and victim machine can be used to propagate the threats to other resources in the victims network[18].

III. TOOLS USED

The works proposed involves the use of two tools namely: MSI Simple Phish and Super Phisher.

A. *MSI Simple Phish:*

MSI Simple Phish is a free tool that provides a simple, safe and effective mechanism for security teams and administrators to run their own phishing tests inside their organization. They simply install the application on a server or workstation and create a url email/sms/etc. campaign to entice users to visit the site. They can encode the URLs, mask them, or shorten them.

It is also used to host phishing websites. For our work, we have used this tool for hosting the created phishing websites.

B. *Super Phisher:*

Super Phisher is an excellent and simple tool to generate pishing sites. It can create phishing pages for any website like Facebook, Gmail, Yahoo, Hotmail etc by using this phisher creator.

In our work, we are going to use this tool for creating the phishing website for Gmail and then redirecting the victim to the google drive where the victim's desired file is present.

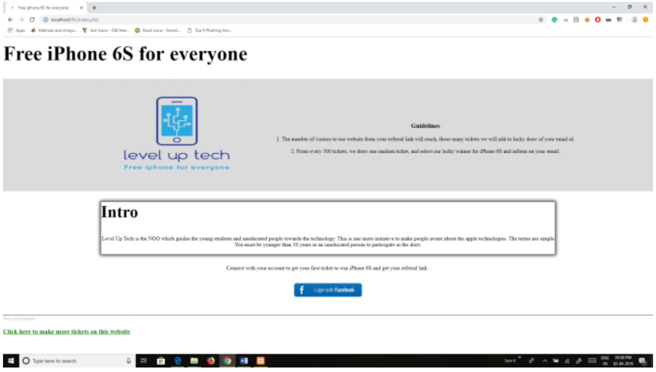
IV. MOTIVATION AND CONTRIBUTION – PROPOSED MECHANISM

A. *Phishing users using Refer and Earn Programme*

A referral program is a marketing tool where you reward your customer to refer your business to a friend/colleague. A refer-and-earn program can help you multiply your business, raise brand awareness and increase your marketing ROI.

There are different types of referral programs like Implied referrals, Tangible referrals, Community referrals and Direct Referrals. For our work, we are using the direct referral programme. A direct referral rewards program is where an existing customer helps sign up another new customer and both get a reward. This is by far, the most popular form of referral program.

For our work, we created a phishing website and hosted it using MSI Simple Phish tool which lures customers by displaying a message that they have won an iphone 6s. To get the reward, the customers have to sign in using their Facebook ID and get their own referral link which they have to share with the other users who can be their friends etc by various means like spamming or sharing it in WhatsApp groups in order to increase their chances of winning.



Free iPhone 6S for everyone

Guidelines

1. The number of visitors to our website from your referral link will reach, those many tickets we will add to lucky draw of your email id.
2. From every 500 tickets, we draw one random ticket, and select our lucky winner for iPhone 6S and inform on your email.

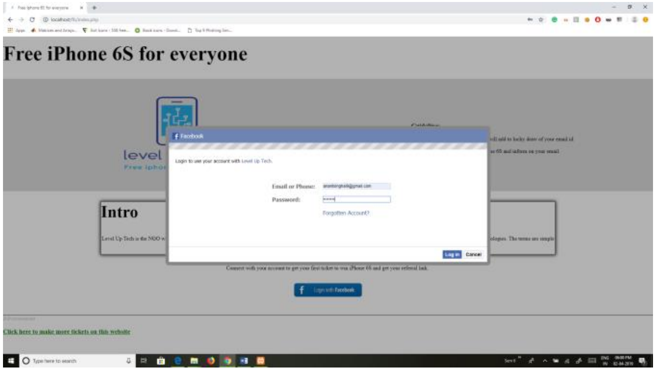
Intro

Level Up Tech is the NGO which guides the young students and uneducated people towards the technology. This is one more initiative to make people aware about the apple technologies. The terms are simple. You must be younger than 30 years or an uneducated person to participate in the draw.

Connect with your account to get your first ticket to win iPhone 6S and get your referral link.

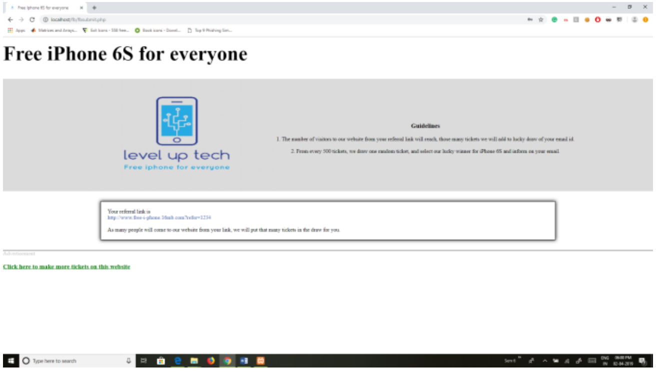
Click here to make more tickets on this website

As soon as the user logs in using their fb ID and password, it gets saved into the hacker's databasse and then the user is provided with a referral link which he is asked to share among different users in order to increase his chances of winning.



Login to use your account with Level Up Tech.

Email or Phone:
Password: •••••



Free iPhone 6S for everyone

Guidelines

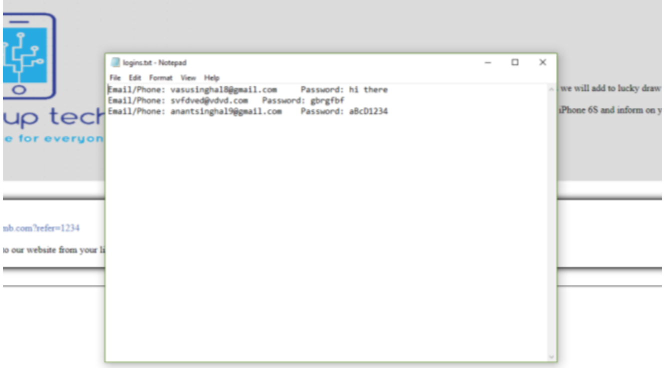
1. The number of visitors to our website from your referral link will reach, those many tickets we will add to lucky draw of your email id.
2. From every 500 tickets, we draw one random ticket, and select our lucky winner for iPhone 6S and inform on your email.

Your referral link is
http://www.free-i-phone.16mb.com?refer=1234

As many people will come to our website from your link, we will put that many tickets in the draw for you.

Click here to make more tickets on this website

This referral link directs the referred users to this phishing page and similarly, their fb password is also stored in the attacker's database.



logins.txt - Notepad

```
Email/Phone: vasusinghal8@gmail.com     Password: hi there
Email/Phone: svfdved@vdvd.com   Password: gbrgfbf
Email/Phone: anantsinghal9@gmail.com     Password: aBcD1234
```

File Edit Format View Help
up tech
e for everyon
we will add to lucky draw
iPhone 6S and inform on y
mb.com?refer=1234
o our website from your li

This is how a user or a group of users can be phished using the refer and earn programme.

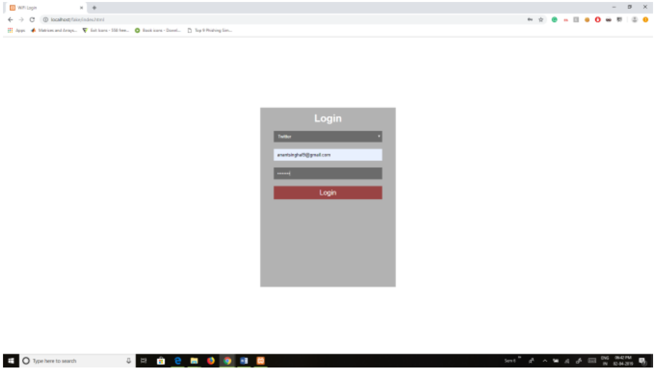
B. *Fake Wifi Login*

Experts say free Wi-Fi connections in public places are usually secure, but more and more criminals are finding ways to lure you onto their rogue connections. When you do, they are collecting everything from passwords to financial information. Ryan says criminals are leveraging available technology to steal information by using devices like a Rogue Access Point. It sends out a signal in popular areas, mimicking a public Wi-Fi hotspot. "If you are not indeed connected to the actual access point that you intend on connecting to, it can be extremely detrimental," Ryan said. Instead of connecting to a public Wi-Fi network, Ryan says hackers are hoping you log onto theirs.

Criminals will redirect you to a fake website, say for example, banking. The webpage looks like a legitimate bank's site, but in reality it is a mock page setup by the hacker. When your login name and password are entered, they could have access to your financial information.
If while you're connected to that rogue AP, it checks mail, they're going to get into that.
Hackers will even be able to obtain your passwords for social media sites.

Many public Wi-Fi networks will ask you to agree with their terms and service before using it. If not, you won't have access. Ryan says if you connect to a network and immediately start browsing, that could be a red flag. Another warning sign is a sluggish connection.

To demonstrate such attack, we have created such scenario by building a phishing website which looks legitimate, just like a public wifi login page. Here the users need to login by any of the social networking websites like Facebook, Twitter, LinkedIn or Google+ to authenticate themselves.

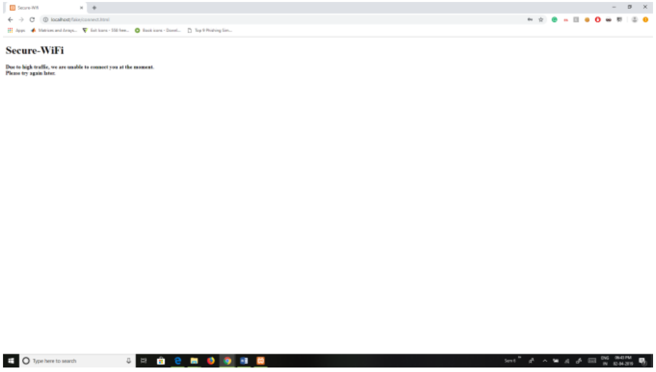


Login

Twitter

anantsinghal9@gmail.com

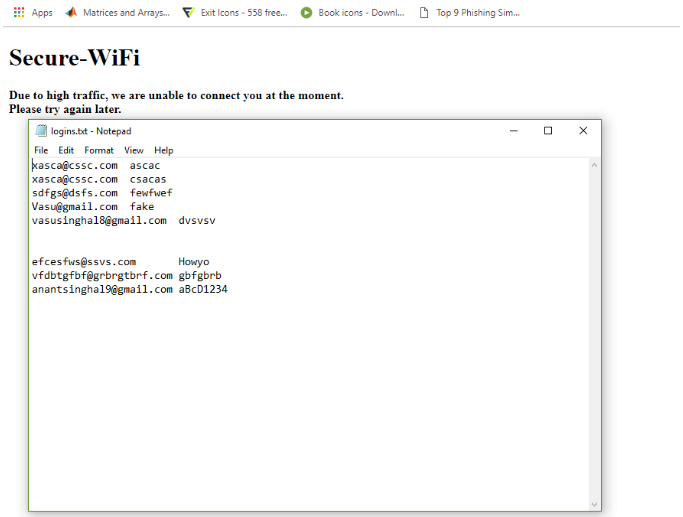
As soon as the user provides the login credentials of any of their social networking account, it gets stored into the attacker’s database and the user is befooled with a message “Due to high traffic, we are unable to connect you at the moment. Please try again later. “



Secure-WiFi

Due to high traffic, we are unable to connect you at the moment.
Please try again later.

And the attacker gets the ID as well as the password of the user in his database.



Secure-WiFi

Due to high traffic, we are unable to connect you at the moment.
Please try again later.

logins.txt - Notepad

```
kasca@cssc.com  ascac
xasca@cssc.com  csacas
sdfgs@dsfs.com  fewfwef
Vasu@gmail.com  fake
vasusinghal8@gmail.com  dvsvsv


efcesfws@ssvs.com       Howyo
vfdbtgfbf@grbrgtbrf.com gbfgbrb
anantsinghal9@gmail.com aBcD1234
```

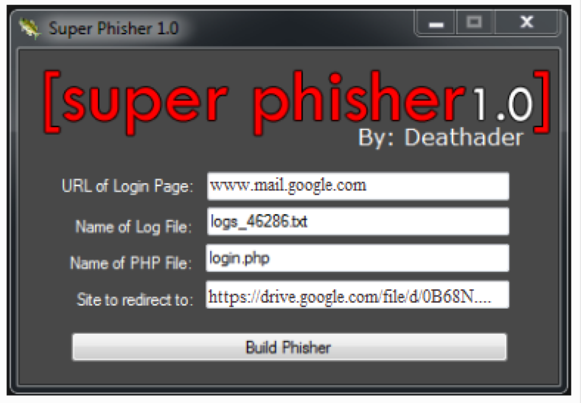
To protect yourself from this attack, it is advised to go into your device network settings and forget any previous public networks. This way, if you did connect to a rogue access point in the past, you will not automatically connect to them in the future. Also, turn off the Wi-Fi on your phone or tablet when not in use.

C. *Redirecting the user*

These days many of the software programs, games or movies etc are made available over the internet free of cost by the hackers. They are known as the pirated softwares. Piracy is strictly illegal and is punishable according to the law.

Many of the pirated websites earn money by selling user data without the user's consent. They asks users to sign in to their website in order to download a particular software or movie free of cost. When the user signs in on their website, the login credentials gets stored into the attacker's database and the user is just redirected to the link having the user desired file. And that's how a user is befooled and results in loss and leakage of sensitive data to the attacker.

For our work, we have created a phishing website for Gmail using the Super Phisher tool.



URL of Login Page: www.mail.google.com

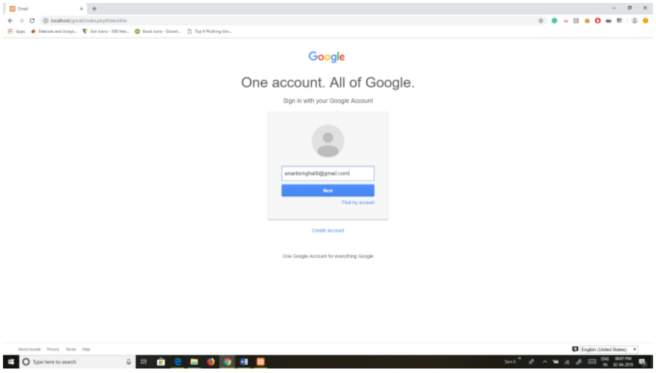
Name of Log File: logs_46286.txt

Name of PHP File: login.php

Site to redirect to: https://drive.google.com/file/d/0B68N....

We get the Gmail phishing site. Consider a scenario where a user wants to download some pirated game from a particular website. The website asks the user to first sign in using Facebook or Gmail (for faster login). The user signs in using Gmail and all his information gets stored into the attacker's database. The website redirects the user to the link where the actual pirated game is present. The user downloads the game unaware of the fact that he has been phished and his Gmail ID has been compensated.

The phishing website for Gmail:



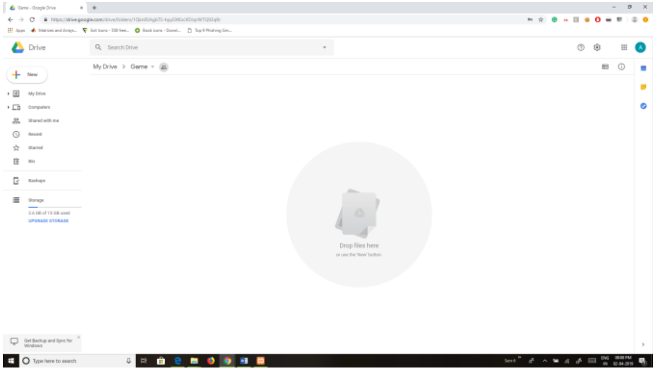
One account. All of Google.

Sign in with your Google Account

anantsinghal9@gmail.com

One Google Account for everything Google

The user signs in to Gmail using his login credentials. And then, he is redirected to the link where the pirated game is present:



References

[1] F. Mouton, M. Malan, L. Leenen and H.S. Venter, "Social Engineer Attack Framework," IEEE Conference on Information Security for South Africa , 2014, pp. 1 - 9.

[2] J. Allen, L. Goman, M. Green, P. Ricciardi, C. Sanabria and Steve Kim, "Social Network Security Issues: Social Engineering and Phishing Attack ," CSIS, Pace University , 2012, pp. B1.1 - B1.7.

[ ] M. Bezuidenhout, F. Mouton and H. S. Venter," Social Engineering Attack Detection Model: SEADM," IEEE Conference on Information Security for South Africa, 2010, pp. 1 - 8,

[4] S. H. Gunawardena, D. Kulkarni and B. Gnanasekaraiyer, "A steganography-based Framework to Prevent Active Attacks during User Authentication," 8thInternational Conference on Computer science & Education (ICCSE), 201 , pp. 8 - 88.

[5] R. S. Rao and S. T. Ali," A Computer Vision Technique to Detect Phishing Attacks," Fifth International Conference on Communication System and Network Technologies, 2015, pp. 596 - 601.

[6] C.handnogy and P.willson, "Social Engineering: The Art of Human Hacking," Wiley, 2010

[7] J. Chen and C. Guo, "Online Detection and Prevention of Phishing Attack", First International Conference on Communication and Networking in china, chinacom06, 2006, pp. 1 – 7.

[8] B. Zhang, Y. Jiao,Z. Ma, Yongchen Li and Junchao Zhu "An Efficient Image Matching Method using Speed Up Robust Features," IEEE international Conference on Mechatronicsand Automation(ICMA), 2014, pp. 55 -558.

[9] H.Bay, T.Tuytelaars and L. Van Gool, "SURF: Speeded UP robust Features." European Conference on Computer Vision (ECCV), Springer Berlin,2006, pp. 400-417.

[10] F. Mouton, L. Leenen, M. M. Malan and H.S. Venter, " Towards an Ontological Model Defining the Social Enginee

ring Domain" 11th Human Choice and Computers International Conference, Turku , pp. 266 - 279, July 2014

[11] M. Fujikawa and M. Nishigaki, "A Study of Prevention for Social Engineering Attacks using Real/Fake Organization‟s Uniforms," Sixth International Conference on Availability, Reliability and Security , 2011, pp. 597602

[12] searchsecurity.techtarget.com/definition/emailspoofing {accessed.online 10 October, 2015}

[1] https://en.wikipedia.org/wiki/hacker {accessed. online 28 October, 2015}

[14] https://blog.returnpath.com/10-tips-on-how -to-identifya-phishing-or-spoofing-email-v2 {accessed. online 2 December, 2015}

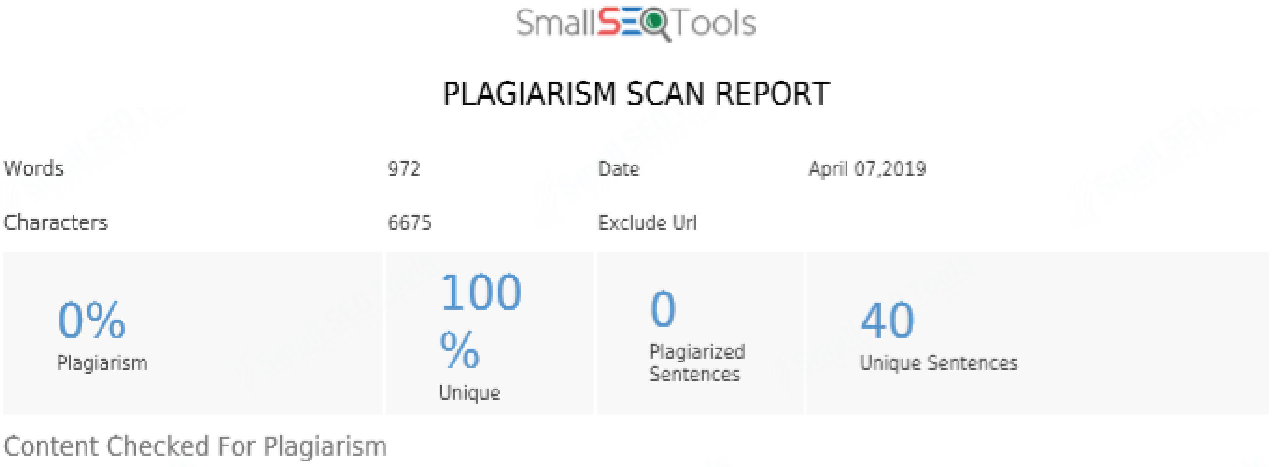
[15] searchsecurity.techtarget.com/definition/Trojan-Horse {accessed. online 12 November, 2015}

[16] [www.wikihow.com/prvent-hacking {accessed. online 12 January, 2016}

[17] U. Naresh, U. VidyaSagar and C. V. Madhusudan Reddy, "Intelligent Phishing Website Detection and Prevention System by Using Link Guard Algorithm" IOSR Journal of Computer Engineering (IOSR-JCE) 201 , vol. XIV, pp 28- 6

[18] www.wikihow.com/Tell-if-Your-Computer-Is-Infectedby-a-Trojan-Horse {accessed. Online 17 January , 2016}

V. PLAGIARISM REPORT



SmallSEOTools

PLAGIARISM SCAN REPORT

Words	972	Date	April 07,2019
Characters	6675	Exclude Url	

0% Plagiarism	100 % Unique	0 Plagiarized Sentences	40 Unique Sentences

Content Checked For Plagiarism